CLAIMS

1. A method comprising:

receiving an event, the event comprising a data section containing a set of strings each containing an event field;

referencing a definition table to determine locations of event fields in the data section of the event; and

storing the event fields in a database record corresponding to event field locations referenced from the definition table.

2. The method as recited in Claim 1, wherein the event fields are in the form of a data value.

3. The method as recited in Claim 1, further comprising generating the definition table by:

selecting one or more specific types of event fields from a event schema;

ascertaining locations of the specific types of event fields in the event schema; and

storing the locations of the specific types of event fields in the definition table.

4. The method as recited in Claim 1, wherein a portion of the set of strings pertains to a security sensitive transaction.

5. The method as recited in Claim 1, wherein the event is received from an event log.

6. The method as recited in Claim 1, wherein the event further comprises an event header section that includes an event identification indicating a select one of a plurality of different types of events.

7. One or more computer-readable media comprising computer-executable instructions that, when executed, perform the method as recited in claim 1.

8. A method comprising:

receiving an event that contains, respectively, an event identification indicating a select one of a plurality of different types of events and one or more sets of strings with each string containing an event field;

identifying the event indication in the event;

locating an entry in a definition table corresponding to the event identification of the received event;

from the located entry of the event in the definition table, the located entry containing locations of types of event fields for the event, using the definition table as a reference to locate event fields in the received event; and

for the received event, storing the located event fields in records of an event database corresponding to the types of event fields.

9. The method as recited in Claim 8, wherein the values in the event fields are in the form of a data value.

10. The method as recited in Claim 8, further comprising:

generating the definition table by:

selecting one or more specific types of event fields from a event schema;

ascertaining locations of the specific types of event fields in the event schema; and

storing the locations of the specific types of event fields in the definition table.

11. The method as recited in Claim 8, wherein a portion of the set of strings pertains to a security sensitive transaction.

12. The method as recited in Claim 8, wherein the event is received from a security log.

13. One or more computer-readable media comprising computer-executable instructions that, when executed, perform the method as recited in claim 8.

14. A system for maintaining records of events comprising:

an event receiver module, configured to receive an event that contains, respectively, an event identification indicator and strings containing event fields each specifying a different component aspects of the event; and

an event-processing module, configured to reference an event definition table to determine locations of event fields in the event, and store the event fields

in a record of a database according to the different component aspect specified by the event field.

15. The system as recited in Claim 14, further comprising a computer that maintains the event receiver module and the event-processing module.

16. The system as recited in Claim 14, further comprising a client computer that performs certain actions that are recorded as an event.

17. The system as recited in Claim 14, wherein one or more the event pertains to a security sensitive transaction.

18. The system as recited in Claim 14, wherein one or more of the event fields pertain to a client logging-on to a network.

19. The system as recited in Claim 14, wherein one or more of the event fields pertain to a client opening a file.

20. The system as recited in Claim 14, wherein one or more of the event fields pertain to a client performing certain application level tasks.

21. The system as recited in Claim 14, wherein one or more of the event fields pertain to a client administering passwords.

22. The system as recited in Claim 14, wherein one or more of the event fields pertain to a client changing passwords.

23. The system as recited in Claim 14, wherein one or more of the event fields pertain to a client accessing a particular object.

24. The system as recited in Claim 14, further comprising a definition-module, configured to generate a definition table by:

selecting one or more specific types of event fields from a event schema;

ascertaining locations of the specific types of event fields in the event schema; and

storing the locations of the specific types of event fields in the definition table.

25. One or more computer-readable media having stored thereon a computer program that, when executed by one or more processors, causes the one or more processors to:

receive an event that contains, respectively, an event identification indicating a select one of a plurality of different types of events and one or more sets of strings with each string containing an event field;

identify the event indication in the event;

locate an entry in a definition table corresponding to the event identification of the received event;

from the located entry of the event in the definition table, the located entry containing locations of types of event fields for the event, use the definition table as a reference to locate event fields in the received event; and

for the received event, store the located event fields in records of an event database corresponding to the types of event fields..

26. One or more computer-readable media as recited in Claim 25, that when executed by one or more processors, further causes the one or more processors to:

generate the event definition table by:

selecting one or more specific types of event fields from a event schema;

ascertaining locations of the specific types of event fields in the event schema; and

storing the locations of the specific types of event fields in the definition table.

27. A system for storing events, comprising:

client computers, configured to generate events that contain, respectively, an event identification indicator and one or more strings, the strings containing event fields;

an event definition table specifying locations of the event fields; and

means for storing the one or more event fields from generated events in records of a database appurtenant to the locations specified by the event definition table.

28. The system as recited in Claim 27, further comprising a means for generating the event definition table comprising:

means for selecting one or more specific types of event fields from a event schema;

means for ascertaining locations of the specific types of event fields in the event schema; and

means for storing the locations of the specific types of event fields in the definition table..

29. The system as recited in Claim 27, wherein the means for storing the one or more event fields in the database record is performed by an event-processing module of a computer.

30. The system as recited in Claim 27, wherein the event identification indicator identifies a type of security sensitive event performed by the computer.

31. One or more computer-readable media comprising computer executable instructions that, when executed, direct a computer to:

generate events that contain, respectively, an event identification and one or more event descriptions, the event descriptions containing one or more values in the event fields, and store the events strings in a log when a security sensitive event is performed; and

store the events in a database in a manner to enable values in the event fields to be independently searched through the use of an event definition table containing mappings of the event descriptions for each event identification, the

mappings including the locations of one or more values in the event fields contained within the event descriptions.

32. One or more computer-readable media as recited in Claim 31, further comprising computer executable instructions that, when executed, direct the computer to parse the event descriptions to identify one or more values in the event fields.

33. One or more computer-readable media as recited in Claim 31, further comprising computer executable instructions that, when executed, direct the computer to generate the event definition table by:

selecting one or more value types from the event;

ascertaining locations of the values in the event fields in the event that correspond to the one or more selected value types; and

storing the location of the values in the event fields in fields of the definition table that corresponding to the one or more selected value types.